TITLE 11 CONSUMER PROTECTION DIVISION OF THE OFFICE OF THE ATTORNEY GENERAL

Proposed Rule
LSA Document #20-366

DIGEST

Adds 11 IAC 4 to establish safe harbor standards for a data base owner's duty to implement and maintain a data security plan, and set out procedures for notifying the attorney general and implementing corrective action in case of a breach of security of data. Effective 30 days after filing with the Publisher.

IC 4-22-2.1-5 Statement Concerning Rules Affecting Small Businesses

11 IAC 4

SECTION 1. 11 IAC 4 IS ADDED TO READ AS FOLLOWS:

ARTICLE 4. DATA PRIVACY

Rule 1. Security Breaches

11 IAC 4-1-1 Definitions

Authority: IC 4-6-9-8
Affected: IC 24-4.9-2; IC 24-4.9-3-3.5

Sec. 1. (a) The definitions set forth in IC 24-4.9-2, as supplemented by the additional definitions set forth in this section, apply throughout this article.

(b) "Breach of the security of data", as defined by IC 24-4.9-2-2, shall be construed interchangeably with "breach of security of data".

(c) "Covered entity" shall be construed interchangeably with "data base owner".

(d) "Data security plan" includes the written policies, procedures, and controls implemented and maintained by a data base owner to protect and safeguard from unlawful use or disclosure personal information of Indiana residents collected and maintained by the data base owner. A data security plan includes both the physical and nonphysical components of the data base owner's policies, procedures, and controls to prevent the breach of security of data.

(Consumer Protection Division of the Office of the Attorney General; 11 IAC 4-1-1)

11 IAC 4-1-2 Duty to implement and maintain a data security plan reasonably designed to prevent a breach of security of data

Authority: IC 4-6-9-8
Affected: IC 24-4.9-3-3.5

Sec. 2. (a) A data base owner's duty to implement and maintain reasonable procedures under IC 24-4.9-3-3.5(c) includes the duty to implement and maintain a data security plan that is reasonably designed to protect and safeguard from unlawful use or disclosure personal information of Indiana residents collected and maintained by the data base owner.

(b) The failure to implement and maintain a data security plan that is reasonably designed to prevent a breach of security of data constitutes a deceptive act.

(Consumer Protection Division of the Office of the Attorney General; 11 IAC 4-1-2)

11 IAC 4-1-3 Duty to take appropriate corrective action following a breach of security of data

Authority: IC 4-6-9-8
Affected: IC 24-4.9-3; IC 24-4.9-4-1

Sec. 3. (a) The duty to take appropriate corrective action under IC 24-4.9-3-3.5(c) includes the following:

(1) The duty to continuously monitor and remediate potential vulnerabilities in a timely fashion as defined by section 4(c) of this rule.

(2) The duty to take reasonable steps to mitigate and prevent the continued unlawful use and disclosure of personal information following any breach of security of data.

(3) The duty to prepare a written corrective action plan following any breach of security of data.

(b) At a minimum, a written corrective action plan must do the following:

(1) Outline the nature and all known or potential causes of the breach with reasonable specificity and citations to applicable technical data.

(2) Identify the precise date and time of the initial breach, and any subsequent breaches, if feasible.

(3) Confirm that corrected measures were implemented at the earliest reasonable opportunity.

(4) Identify the specific categories of personal information subject to unlawful use or disclosure, including the approximate number of individuals affected.

(5) Identify what steps have already been taken to mitigate and prevent the continued unlawful use and disclosure of personal information.

(6) Identify a specific corrective plan to mitigate and prevent the continued unlawful use and disclosure of personal information.

(c) A data base owner shall certify under penalty of perjury to the attorney general that it has developed and implemented a corrective action plan within thirty (30) days of the required disclosure to the attorney general under IC 24-4.9-3-1. The data base owner shall maintain a copy of the current plan, and it must be made available to the attorney general upon request without delay. The attorney general may require that the data base owner submit periodic updates to ensure that the data base owner is taking appropriate corrective action. The attorney general is authorized to conduct random and unannounced audits, and noncooperation is a disqualification for safe harbor under this rule.

(d) Compliance with the disclosure and notification requirements under IC 24-4.9-3 does not, by itself, constitute appropriate corrective action.

(e) The failure to take appropriate corrective action consistent with this section constitutes a deceptive act.

(Consumer Protection Division of the Office of the Attorney General; 11 IAC 4-1-3)

11 IAC 4-1-4 Safe harbor for reasonable measures taken to prevent breach of security of data

Authority: IC 4-6-9-8
Affected: IC 24-4.9-3-3.5

Sec. 4. (a) Procedures adopted under IC 24-4.9-3-3.5(c) are presumed reasonable if the procedures comply with this section, including one (1) of the following applicable standards:

(1) A covered entity implements and maintains a cybersecurity program that complies with the National Institute of Standards and Technology (NIST) cybersecurity framework and follows the most recent version of one (1) of the following standards:

(A) NIST Special Publication 800-171.

(B) NIST SP 800-53.

(C) The Federal Risk and Authorization Management Program (FedRAMP) security assessment framework.

(D) International Organization for Standardization/International Electrotechnical Commission 27000 family - information security management systems.

(2) A covered entity is regulated by the federal or state government and complies with one (1) of the

following standards as it applies to the covered entity:

(A) The federal USA Patriot Act (P.L. 107-56).

(B) Executive Order 13224.

(C) The federal Driver's Privacy Protection Act (18 U.S.C. 2721 et seq.).

(D) The federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

(E) The federal Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104-191).

(3) A covered entity complies with the current version of the payment card industry data security standard in place at the time of the breach of security of data, as published by the Payment Card Industry Security Standard Council.

(b) If a new version of a standard listed in subsection (a) is released, the data base owner shall implement the standard by the effective date; or, if no effective date is provided, within one (1) year of the proposed standard first being published.

(c) The data security plan incorporates monitoring of vulnerabilities as tracked by NIST National Vulnerability Database, and for each vulnerability that is ranked as critical, the data base owner shall commence remediation planning within twenty-four (24) hours after the vulnerability has been rated as critical and shall apply the remediation within one (1) week after the vulnerability has received a critical rating.

(d) A revised risk assessment is conducted no less than annually, and the data security plan is revised to address the updated risks.

(e) The data base owner bears the burden of demonstrating that its data security plan was reasonably designed, implemented, and executed to prevent the breach of security of data. Upon such a showing, the data base owner will not be subject to a civil action from the office of the attorney general arising from the breach of security of data. The office of the attorney general shall make a determination consistent with the requirements of this section.

(Consumer Protection Division of the Office of the Attorney General; 11 IAC 4-1-4)

11 IAC 4-1-5 Unreasonable delay in disclosing a breach of security of data

Authority: IC 4-6-9-8
Affected: IC 24-4.9-3-1; IC 24-4.9-3-3.5

Sec. 5. (a) A data base owner's duty of disclosure under IC 24-4.9-3 will be deemed presumptively reasonable if made within thirty (30) days that the data base owner knew, or reasonably should have known, of a breach of security of data.

(b) The particular circumstances of a breach of security of data, or a data base owner's corrective action, may warrant a deviation from the presumption afforded under this section.

(Consumer Protection Division of the Office of the Attorney General; 11 IAC 4-1-5)

11 IAC 4-1-6 Limitation to civil actions initiated under IC 24-4.9-1-1

Authority: IC 4-6-9-8
Affected: IC 24-4.9-1-1

Sec. 6. Nothing in this rule should be construed to limit the Indiana office of the attorney general from enforcing violations of statutes other than IC 24-4.9-1-1, including unfair, abusive, or deceptive acts or omissions, regardless of whether the conduct is related or connected to the breach of security of data.

(Consumer Protection Division of the Office of the Attorney General; 11 IAC 4-1-6)

11 IAC 4-1-7 Limitation of cause of action

Authority: IC 4-6-9-8

Affected: IC 24-4.9-1-1

Sec. 7. This rule shall not be construed to provide a cause of action to any public or private entity or consumer, including a class action, with respect to any act or practice regulated under this rule.

(Consumer Protection Division of the Office of the Attorney General; 11 IAC 4-1-7)

Notice of Public Hearing

Posted: 10/07/2020 by Legislative Services Agency
An html version of this document.